



Odd Perfect Numbers: A Triptych

WILLIAM DUNHAM 

Number theory occupies a strange corner of mathematics. G. H. Hardy (1877–1947) captured this in describing the appeal of the whole numbers:

There is a great deal of mathematics the purport of which is quite impossible for any amateur to grasp, and which, however beautiful and important it may be, must always remain the possession of a narrow circle of experts. It is a peculiarity of the theory of numbers that much of it could be published broadcast, and would win new readers for the *Daily Mail*.

To be sure, the whole numbers have a simplicity not shared by, say, the irrationals. Yet this simplicity is deceptive, for number theory is awash in challenges. As Hardy put it in describing these challenges, “There is no one so blind that he does not see them, and no one so sharp-sighted that his vision does not fail” [4].

Examples abound of easy-to-state problems in number theory that have frustrated generations of mathematicians. One of the greatest of these is the subject at hand: odd perfect numbers.

Every schoolchild knows what an odd number is. And we recall that a whole number is *perfect* if it is the sum of its proper whole number divisors. Here “proper” means “smaller than the number itself.” The first example is 6, for its proper divisors are 1, 2, and 3, and $1 + 2 + 3 = 6$. The next is 28, which is perfect because $1 + 2 + 4 + 7 + 14 = 28$. What could be simpler?

The Greek mathematician Nicomachus (ca. 100) was smitten by this concept and asserted that perfect numbers—like all “fair and excellent things”—are rare, whereas “ugly and evil ones are widespread” [6, p. 209]. For him, perfection set a high bar, numerically and aesthetically.

The two perfect numbers shown above are even, and therein lies the fundamental question: Are there any odd perfect numbers? The answer, of course, must be either yes or no. If there are odd perfect numbers, we need only find one; if there are not, we must give a proof that no such thing can possibly exist. After centuries of effort, mathematicians can do neither.

Intuitively, there is a compelling reason to be pessimistic about their existence. When we add the proper divisors of smallish odd numbers, the sum always seems to come up short of the number itself. The odd numbers 3, 5, and 7 are all primes, whose only proper divisors are 1. With 9, we get 1 and 3 as a pair of proper divisors, but $1 + 3 = 4 < 9$. And so it goes through the first dozen odds, and the first fifty odds, and the first hundred odds. In each case, the sum of the proper divisors is less than the number, and so these odds are not perfect.

This phenomenon holds right up through the odd number 943, the sum of whose proper divisors is $1 + 23 + 41 = 65 < 943$. After having considered 472 consecutive odds and finding that in every case, the sum of the proper divisors is less than the number, we are ready to conjecture that the sum of the proper divisors of an odd number will always be less than the number.

But the next odd number is 945, and the sum of its proper divisors is a robust

$$1 + 3 + 5 + 7 + 9 + 15 + 21 + 27 + 35 + 45 + 63 + 105 + 135 + 189 + 315 = 975 > 945.$$

Our conjecture is wrong. An odd number can have proper divisors whose sum exceeds the number, and it can have proper divisors whose sum falls short. Why, then, can’t the sum of its proper divisors exactly equal that number?

Why indeed?

In an attempt to chip away at this mystery, mathematicians have proved a host of theorems that begin, “If N is an odd perfect number, then ...” Such a theorem, of course, does nothing to confirm or deny the existence of such a number. Rather, it establishes what an odd perfect number must look like—if there is one.

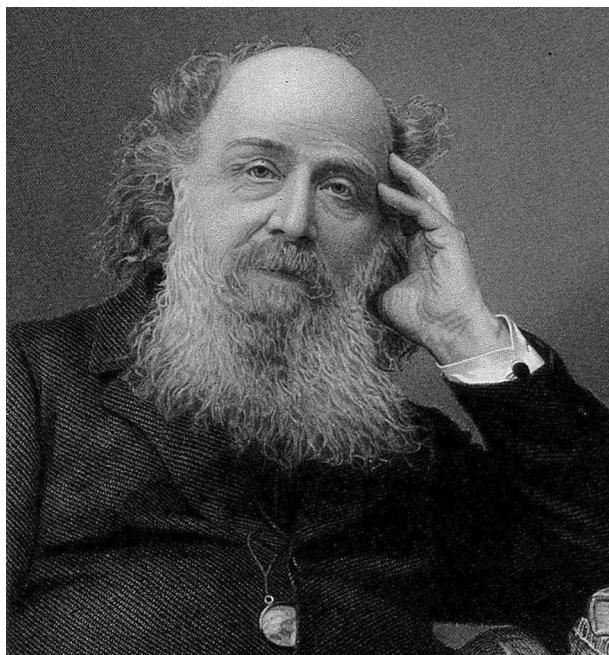
In this article, we examine three proofs of this nature. Like a three-paneled triptych from medieval art, these are related and jointly tell a story. But whereas triptychs from the Old Masters told a religious tale, ours is a mathematical one.

Our first “panel” comes from Leonhard Euler (1707–1783) in the eighteenth century; the other two are from J. J.

Sylvester (1814–1897) in the nineteenth. These are simple, elegant arguments that require little prior knowledge yet provide truly unintuitive insights into the structure of an odd perfect number. And they demonstrate—if further demonstration is necessary—why the history of mathematics can be such a rewarding enterprise.



Leonhard Euler (*cropped and reproduced under Creative Commons license*).



J. J. Sylvester (*cropped and reproduced under Creative Commons license*).

To follow these arguments, we need a few preliminaries. One is the undisputed workhorse of number theory: unique factorization. This says that every whole number greater than 1 can be factored into a product of primes in one and only one way.

Next, we need the σ -function, defined by Euler in 1750 as follows [2]:

$\sigma(n)$ is the sum of all whole number divisors of n .

For instance, $\sigma(3) = 1 + 3 = 4$ and $\sigma(6) = 1 + 2 + 3 + 6 = 12$. Clearly, the sum of the *proper* divisors of n is $\sigma(n) - n$, and so N is perfect if and only if $\sigma(N) = 2N$.

Beyond its definition, Euler's σ -function has two properties we shall use in the proofs to come. First, $\sigma(M) \geq M$. This is because every M has at least one divisor, namely M itself. Second, and more significantly, if a and b are relatively prime, then $\sigma(ab) = \sigma(a)\sigma(b)$. So

$$\sigma(6) = \sigma(2 \cdot 3) = \sigma(2) \cdot \sigma(3) = 3 \cdot 4 = 12,$$

as we saw above. The proof of this property can be found in any number theory text.

We now consider four elementary lemmas.

LEMMA 1: If p is a prime and if r is a whole number, then

$$\sigma(p^r) = 1 + p + p^2 + \cdots + p^r.$$

PROOF: This is immediate, because the only divisors of a power of a prime are themselves powers of that prime.

LEMMA 2: If p is an odd prime, then $\sigma(p^r)$ is even if r is odd, and $\sigma(p^r)$ is odd if r is even.

PROOF: By Lemma 1, $\sigma(p^r) = 1 + p + p^2 + \cdots + p^r$, an expression with $r+1$ odd summands.

LEMMA 3: If r is odd and if the prime p is one less than a multiple of 4, then 4 divides $\sigma(p^r)$. (Following custom, we shall express this last statement as $4|\sigma(p^r)$, where $a|b$ means that the whole number a divides the whole number b , that is, that a is a factor of b .)

PROOF: We assume $p = 4k - 1$ for some whole number k . Lemma 1 shows that $\sigma(p^r) = 1 + p + p^2 + \cdots + p^r$, the sum of an even number of terms because r is odd. We can pair these to get

$$\begin{aligned} \sigma(p^r) &= (1 + p) + p^2(1 + p) + p^4(1 + p) + \cdots + p^{r-1}(1 + p) \\ &= (1 + p)[1 + p^2 + p^4 + \cdots + p^{r-1}]. \end{aligned}$$

But $1 + p = 1 + (4k - 1) = 4k$. Therefore, $4|1 + p$, and so $4|\sigma(p^r)$ as well.

LEMMA 4: If p is an odd prime and if r is one less than a multiple of 4, then $4|\sigma(p^r)$.

PROOF: Here we assume $r = 4m - 1$. In this case,

$$\begin{aligned}\sigma(p^r) &= 1 + p + p^2 + \cdots + p^r = 1 + p + p^2 + \cdots + p^{4m-1} \\ &= (1 + p + p^2 + \cdots + p^{2m-1}) \\ &\quad + p^{2m}(1 + p + p^2 + \cdots + p^{2m-1}) \\ &= (1 + p + p^2 + \cdots + p^{2m-1})(1 + p^{2m}).\end{aligned}$$

These two factors are even because each is the sum of an even number of odd terms (i.e., of $2m$ and 2 terms, respectively). With each factor being divisible by 2, their product is divisible by $2 \times 2 = 4$. That is, $4|\sigma(p^r)$.

Now we begin our historical journey in earnest. Throughout, we shall assume that N is an odd perfect number. The goal is to follow Euler and Sylvester in establishing conditions about the structure of N .

THEOREM 1 (Euler): An odd perfect number can be written as $N = p^r M^2$, where p is a prime of the form $p = 4k + 1$, the exponent is of the form $r = 4\lambda + 1$, and M and p are relatively prime [3].

PROOF: We begin by factoring N into primes, obtaining the decomposition

$$N = a^n b^m c^q \cdots d^s,$$

where a, b, c, \dots, d are distinct primes, all of which must be odd. It follows that $\sigma(N) = \sigma(a^n)\sigma(b^m)\sigma(c^q)\cdots\sigma(d^s)$, and because N is perfect, we know that

$$2a^n b^m c^q \cdots d^s = 2N = \sigma(N) = \sigma(a^n)\sigma(b^m)\sigma(c^q)\cdots\sigma(d^s).$$

Note that on the left-hand side of the equality, there is a lone 2 among all the prime factors. Because this product is equal to $\sigma(N)$, it follows from unique factorization that $\sigma(N)$ is divisible by 2 but not by 4.

But there is more to be said. Exactly one of the factors on the far right must be even, and all the others must be odd. Let us designate by p the prime for which $\sigma(p^r)$ is even. By Lemma 2, we know that r is an odd exponent. By the same lemma, all of the other primes on the right must have even exponents. That means that the product of these other prime powers can be written as a perfect square, e.g., $b^4 c^6 d^2 = (b^2 c^3 d)^2$.

Putting this together, we see that if N is an odd perfect number, then

$$N = p^r M^2, \quad (*)$$

where p is an odd prime, r is an odd exponent, and M is a whole number relatively prime to p .

So far, so good. But more must be done, for Euler's characterization further specified the nature of p and r .

(A) For this situation, p must be of the form $4k + 1$.

PROOF: If not, then the odd prime p is equal to $4k - 1$. By Lemma 3, we know that 4 divides $\sigma(p^r)$. But then 4 divides

$\sigma(p^r) \cdot \sigma(M^2) = \sigma(N)$, by (*). This contradicts the observation that $\sigma(N)$ is divisible by 2 but not by 4. Consequently, $p = 4k + 1$, confirming (A).

(B) For this situation, r must be of the form $4\lambda + 1$.

PROOF: If not, then the odd number r must look like $4\lambda - 1$. By Lemma 4, $4|\sigma(p^r)$, and so 4 is a divisor of $\sigma(p^r) \cdot \sigma(M^2) = \sigma(N)$, which brings us to the same contradiction as in (A). Thus r takes the form $r = 4\lambda + 1$.

Combining (A), (B), and (*), we reach Euler's structure theorem for an odd perfect number: $N = p^{4\lambda+1} M^2$, where p is a prime of the form $4k + 1$ that is relatively prime to M .

Q. E. D.

Among other things, Euler's result says that for an odd perfect number, every prime factor of the form $4m - 1$ must be raised to an even power. So if 7 is a prime factor of an odd perfect number, it can appear in the factorization as 7^2 or 7^4 , but not as 7^3 or 7^5 or, for that matter, as 7 alone.

With this proof, Euler determined the broad structure of an odd perfect number and in the process eliminated an infinitude of odd numbers from consideration. Of course, infinitely many odd numbers were not eliminated and remained as candidates for perfection. But it was a first step.

We now jump to the nineteenth century to follow J. J. Sylvester as he picks up the scent. The key tool in his arguments is again the Euler σ -function.

Before proceeding, we note that for a prime p ,

$$\frac{\sigma(p^r)}{p^r} = \frac{1 + p + p^2 + \cdots + p^r}{p^r} = 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots + \frac{1}{p^r}.$$

So if $r \geq 1$, then $\frac{\sigma(p^r)}{p^r} \geq 1 + \frac{1}{p}$; and if $r \geq 2$, then $\frac{\sigma(p^r)}{p^r} \geq 1 + \frac{1}{p} + \frac{1}{p^2}$.

As a final warm-up for Sylvester's theorems, we prove the following:

THEOREM: A power of an odd prime cannot be perfect.

PROOF: Suppose p^r is perfect, where p is an odd prime. We know that $\sigma(p^r) = 2p^r$, which amounts to $1 + p + p^2 + \cdots + p^{r-1} + p^r = 2p^r$. Therefore,

$$1 = p^r - p^{r-1} - \cdots - p^2 - p = p(p^{r-1} - \cdots - p - 1).$$

It follows that $p \mid 1$, which is impossible because 3 is the smallest of the odd primes. Hence p^r cannot be perfect.

Q.E.D.

This result means that if we seek an odd perfect number, it must have at least two distinct prime factors. In 1888, Sylvester published a clever argument to show that the minimum number of distinct prime factors is in fact three. It is the second panel of our triptych.

THEOREM 2 (Sylvester): An odd perfect number must have at least three distinct prime factors [9, p. 209].

PROOF: Suppose we have an odd perfect number $N = p^r q^s$, where p and q are odd primes with $p < q$. By definition, $\sigma(N) = 2N$, and so

$$\begin{aligned} 2p^r q^s &= \sigma(p^r q^s) = \sigma(p^r) \sigma(q^s) \\ &= (1 + p + p^2 + \cdots + p^r)(1 + q + q^2 + \cdots + q^s). \end{aligned}$$

It follows that

$$\begin{aligned} 2 &= \frac{1 + p + p^2 + \cdots + p^r}{p^r} \cdot \frac{1 + q + q^2 + \cdots + q^s}{q^s} \\ &= \left[1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^r} \right] \cdot \left[1 + \frac{1}{q} + \frac{1}{q^2} + \cdots + \frac{1}{q^s} \right]. \end{aligned}$$

But p is an odd prime, so $p \geq 3$. And q is a *larger* odd prime, so $q \geq 5$. Of course, this means that $1/p \leq 1/3$ and that $1/q \leq 1/5$, and thus

$$2 \leq \left[1 + \frac{1}{3} + \frac{1}{9} + \cdots + \frac{1}{3^r} \right] \cdot \left[1 + \frac{1}{5} + \frac{1}{25} + \cdots + \frac{1}{5^s} \right].$$

If we replace each finite geometric series with its infinite counterpart, we get

$$\begin{aligned} 2 &< \left[1 + \frac{1}{3} + \frac{1}{9} + \cdots \right] \cdot \left[1 + \frac{1}{5} + \frac{1}{25} + \cdots \right] \\ &= \frac{1}{1 - 1/3} \cdot \frac{1}{1 - 1/5} = \frac{3}{2} \cdot \frac{5}{4} = \frac{15}{8}. \end{aligned}$$

We have thereby concluded that $2 < 15/8$, which is absurd. Thus an odd perfect number cannot have just two prime factors. It must have at least three. Q.E.D.

During his career, Sylvester returned to this problem, eventually proving that an odd perfect number must have at least five distinct prime factors [9, pp. 611–614]. But Sylvester found another condition that will complete our triptych. It is an especially unintuitive one.

THEOREM 3 [9, pp. 604–605]: An odd perfect number cannot be divisible by 105.

PROOF: As always, we let N be an odd perfect number, but now we assume, for the sake of contradiction, that $105 \mid N$. Because $105 = 3 \cdot 5 \cdot 7$, we know that N has (at least) these three prime factors. Further, because 3 and 7 are of the form $4m - 1$, Euler's characterization guarantees that each of these must appear with an even exponent. As to the prime 5, we know that its exponent is at least 1, because it is a factor of N .

Thus we have $N = 3^r \cdot 5^s \cdot 7^t \cdot M$, where $r \geq 2$, $s \geq 1$, and $t \geq 2$, and where M is not divisible by 3, 5, or 7. So

$$\begin{aligned} \frac{\sigma(N)}{N} &= \frac{\sigma(3^r)\sigma(5^s)\sigma(7^t)\sigma(M)}{3^r 5^s 7^t M} \\ &= \frac{\sigma(3^r)}{3^r} \cdot \frac{\sigma(5^s)}{5^s} \cdot \frac{\sigma(7^t)}{7^t} \cdot \frac{\sigma(M)}{M} \\ &\geq \left(1 + \frac{1}{3} + \frac{1}{9} \right) \cdot \left(1 + \frac{1}{5} \right) \cdot \left(1 + \frac{1}{7} + \frac{1}{49} \right) \cdot 1, \end{aligned}$$

because $r \geq 2$, $s \geq 1$, and $t \geq 2$ and because $\sigma(M) \geq M$. It follows that

$$\frac{\sigma(N)}{N} \geq \frac{13}{9} \cdot \frac{6}{5} \cdot \frac{57}{49} = \frac{494}{245} > 2.$$

This contradicts the fact that for a perfect number, $\sigma(N) = 2N$. We conclude that an odd perfect number cannot be divisible by 105.

Q.E.D.

Over the years, other facts have been proved about odd perfect numbers. With great subtlety, Sylvester's line of attack has been extended to show that every such number must have at least ten different prime factors [7]. It is known that every odd perfect number has to be greater than 10^{1500} , which guarantees that even the smallest possible candidate is breathtakingly large [8]. And perhaps most strangely, it has been proved that the third-largest prime factor of an odd perfect number must exceed one hundred [5]. This one is especially bizarre, for it tells us something specific about the third largest factor of what could well be a nonexistent entity. This is a bit like knowing the tooth fairy's cousin's middle name.

With so many conditions on the structure of odd perfect numbers, there is a chance that two of them will be incompatible. Were that the case, the nonexistence of an odd perfect number would be established. Indeed, as the increasingly restrictive properties of odd perfect numbers began to pile up, Sylvester observed that

a prolonged meditation on the subject has satisfied me that the existence of [an odd perfect number] – its escape, so to say, from the complex web of conditions which hem it on all sides – would be little short of a miracle [9, p. 590].

But to date, no incompatible properties have appeared. A miracle has yet to be ruled out.

On the one hand, we might regard this situation as a blot on mathematics. After all, a carpenter who can't hammer a nail isn't much of a carpenter. A singer who can't carry a tune isn't much of a singer. Maybe a mathematician who can't answer so elementary a question is similarly deficient. The mathematician E. T. Bell suggested as much when he wrote:

To say that number theory is mistress of its own domain when it cannot subdue a childish thing like odd perfect numbers is undeserved flattery [1, p. 91].

On the other hand, the efforts that have been directed at this problem—although not (yet) conclusive—are ingenious indeed. The results above surely fall into this category. And we must not forget that number theory is, at its heart, a most difficult subject, where even innocent-looking problems can defeat our best efforts. In that spirit, we shall give G. H. Hardy one last word. In spite of the unsolved problems that seem to be mocking us, Hardy believed that number theory has been, and remains, “a continual and inevitable challenge to the curiosity of every healthy mind” [4].

Department of Mathematics
Bryn Mawr College
Bryn Mawr, PA
USA
e-mail: bdunham@brynmawr.edu

REFERENCES

- [1] E. T. Bell. *The Queen of the Sciences*. Williams & Wilkins, 1931.
- [2] L. Euler. “De numeris amicabilibus.” *Opera Omnia*, Ser. 1, Vol. 2, p. 87. (This is listed in the Eneström Index of Euler’s collected works as E-152.)
- [3] L. Euler. *Opera Postuma*. St. Petersburg, 1862, pp. 14–15. (This is listed in the Eneström Index of Euler’s collected works as E-792.)
- [4] G. H. Hardy, “The Theory of Numbers.” *Nature*, September 1922, 385.
- [5] D. E. Iannucci. “The Third Largest Prime Divisor of an Odd Perfect Number Exceeds One Hundred.” *Mathematics of Computation* 69 (2000), 867–879.
- [6] Nicomachus. *Introduction to Arithmetic*, trans. Martin D’ooge. University of Michigan Press, 1938.
- [7] P. P. Nielson. “Odd Perfect Numbers, Diophantine Equations, and Upper Bounds.” *Mathematics of Computation* 84 (2015), 2549–2567.
- [8] P. Ochem and M. Rao. “Odd Perfect Numbers Are Greater than 10^{1500} .” *Mathematics of Computation* 81 (2012), 1869–1877.
- [9] J. J. Sylvester. *The Mathematical Papers of James Joseph Sylvester*, Vol. IV, Chelsea Reprint (1973), pp. 588–589.

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.